INFORMATION DISCLOSURE STATEMENT

1. U.S. Pat. No. 5,606,668, entitled "SYSTEM FOR SECURING INBOUND AND OUTBOUND DATA PACKET FLOW IN A COMPUTER NETWORK," discloses a device for and method of using a packet filter code that contains rules for determining whether or not a received packet should be allowed or denied access to the computer network. U.S. Pat. No. 5,606,668 requires that each packet received in all cases must be processed in accordance with the accept/reject rules. The present invention does not require that each packet received in all cases be analyzed in accordance with accept/reject rules. The processing burden required for each packet received makes the device and method of U.S. Pat. No. 5,606,668 not as efficient or secure as the device and method of the present invention.

2. U.S. Pat. No. 5,623,601, entitled "APPARATUS AND METHOD FOR PROVIDING A SECURE GATEWAY FOR COMMUNICATION AND DATA EXCHANGES BETWEEN NETWORKS," discloses a device for and method of screening data in accordance to the level of security required for the data. U.S. Pat. No. 5,623,601 requires an analysis of all of the received data in accordance with a security profile established by a security administrator. The processing burden required for each datagram received makes the device and method of U.S. Pat. No. 5,623,601 not as efficient and secure as the device and method of the present invention.

3. U.S. Pat. No. 5,802,320, entitled "SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE," discloses a device for and method of screening data without adding any information of any network address pertaining to the screening process. This allows the screening system to function without being identified and, thus, more difficult to target by a hacker. U.S. Pat. No. 5,802,320 requires that each packet received be analyzed in

accordance with accept/reject rules whereas the present invention does not. The processing burden required for each packet received makes the device and method of U.S. Pat. No. 5,802,320 not as efficient and secure as the device and method of the present invention.

4. U.S. Pat. No. 5,826,014, entitled "FIREWALL SYSTEM FOR PROTECTING NETWORK ELEMENTS CONNECTED TO A PUBLIC NETWORK," discloses a device for and method of a firewall. U.S. Pat. No. 5,826,014 requires that each datagram received be analyzed in accordance with accept/reject rules whereas the present invention does not. The processing burden required for each datagram received makes the device and method of U.S. Pat. No. 5,826,014 not as efficient and secure as the device and method of the present invention.

5. U.S. Pat. No. 5,828,844, entitled "INTERNET NCP OVER ATM," discloses a device for and method of a transmitting an IP data packet, ATM signaling, or ATM data. U.S. Pat. No. 5,828,844 does not disclose an efficient and hacker resistant firewall for receiving IP data packets, ATM signaling, and ATM data as does the present invention.

6. U.S. Pat. No. 5,828,833, entitled "METHOD AND SYSTEM FOR ALLOWING REMOTE PROCEDURE CALLS THROUGH A NETWORK FIREWALL," discloses a device for and method of allowing remote procedure calls through a firewall if the application server from which the request was made appears on an access control list. The access control list appears to be manually maintained. There does not appear to be any rules for automatically adding an application server to the access control list based on an analysis of the incoming request as in the present invention.

7. U.S. Pat. No. 5,828,846, entitled "CONTROLLING PASSAGE OF PACKETS OR MESSAGES

VIA A VIRTUAL CONNECTION OR FLOW," discloses a method of a firewall that applies the accept/reject rules to every packet received that concerns flow management (i.e., signaling rather than data) whereas the present invention does not. The processing burden required for each packet received concerning connectivity makes the method of U.S. Pat. No. 5,828,846 not as efficient and secure as the device and method of the present invention.

8. U.S. Pat. No. 5,835,726, entitled "SYSTEM FOR SECURING THE FLOW OF AND SELECTIVELY MODIFYING PACKETS IN A COMPUTER NETWORK," discloses a device for and a method of a firewall that applies the accept/reject rules to every packet received whereas the present invention does not. The processing burden required for each packet received makes the device and method of U.S. Pat. No. 5,835,726 not as efficient and secure as the device and method of the present invention.

9. U.S. Pat. No. 5,835,727, entitled "METHOD AND APPARATUS FOR CONTROLLING ACCESS TO SERVICES WITHIN A COMPUTER NETWORK," discloses a device for and a method of a firewall that applies the accept/reject rules to every datagram received whereas the present invention does not. The processing burden required for each datagram received makes the device and method of U.S. Pat. No. 5,835,727 not as efficient and secure as the device and method of the present invention.

10. The closest prior art to the present invention appears to be the present inventor's own previous work published in a paper entitled "An FPGA-Based Coprocessor for ATM Firewalls," by the IEEE Computer Society, Los Alamitos, CA, on April 16, 1997, in *Proceedings, The 5th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*. The device disclosed in this

publication is the subject of a patent application serial number 09/059,041, filed April 13, 1998, entitled "FIREWALL SECURITY APPARATUS FOR HIGH-SPEED CIRCUIT SWITCHED NETWORKS." The steps of the method disclosed in the above-identified publication are as follows.

The first step is initializing a database and a connection-oriented network approved list, where the database contains rules for allowing and denying access concerning connection-oriented network flows, and where the connection-oriented approved list includes approvals of flows carrying ATM signaling information and ATM data.

The second step is receiving a datagram.

The third step is identifying the type of the datagram (i.e., ATM signaling segment or ATM data segment).

The fourth step is allowing the datagram access to the information processing network, recording that the datagram was allowed access to the information processing network, and comparing the connection request contained therein to the database if the datagram is an ATM signaling segment.

The fifth step is adding the connection request to the connection-oriented network approved list if the connection request is approved by the database and returning to the second step. If the connection request is not approved by the database then return to the second step without recording anything on the approved list.

The sixth step is allowing the datagram access to the information processing network, recording that the datagram was allowed access to the information processing network, and returning to the second step if the datagram is an ATM data segment and is on the connection-oriented network approved list.

The seventh step is discarding the datagram, recording that the datagram was denied access to the information processing network, and returning to the second step if the datagram is an ATM data segment and is not on the connection-oriented network approved list.

The device that implements the method disclosed in the above-identified publication includes a flow management unit, having a first input/output bus for receiving a flow, having a second input/output bus for transmitting a flow, and having a third input/output bus. A connection-oriented approved list storage unit has a first input/output bus and a second input/output bus. A connection-oriented flow processor is connected to the input/output bus of the connection-oriented approved list storage unit and is connected to the third input/output bus of the flow management unit. A flow command processor is connected to the first input bus of the connection-oriented approved list storage unit, is connected to the third input/output bus of the flow management unit, and has an input/output bus. A connection-oriented (e.g., ATM) signaling flow processor is connected to the input/output bus of the flow command processor and has an input/output bus. A connection-oriented signaling address database unit is connected to the input/output bus of the connection-oriented signaling flow processor. A memory management unit is connected to the third input/output bus of the flow management unit and has an input/output bus. A memory unit is connected to the input/output bus of the memory management unit.

The method and device disclosed in the above-identified publication are each a firewall that only processes connection-oriented signaling segments and connection-oriented data segments. The inventors of the present invention improved upon their work by inventing a device and method that processes connectionless network segments (e.g., IP packet segments) contained within connection-oriented network cells (e.g., ATM cells).